RECEIVED
CENTRAL FAX CENTER
NO. 4741 P. 1
NOV 13 2006

ZILKA-KOTAB
PC
ZILKA, KOTAB & FEECE™

100 PARK CENTER PLAZA, SUITE 300
SAN JOSE, CA 95113

TELEPHONE (408) 971-2573
FAX (408) 971-4660

FAX COVER SHEET

Date:	November 13, 2006	**Phone Number**	**Fax Number**
To:	Board of Patent Appeals		(571) 273-8300
From:	Kevin J. Zilka		

Docket No.: NAI1P345/01.239.01 **App. No: 10/068,280**

Total Number of Pages Being Transmitted, Including Cover Sheet: 34

Message:

Please deliver to the Board of Patent Appeals.

Thank you,

Kevin J. Zilka

☐ *Original to follow Via Regular Mail* X *Original will Not be Sent* ☐ *Original will follow Via Overnight Courier*

****
The information contained in this facsimile message is attorney privileged and confidential information intended only for the use of the individual or entity named above. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution or copy of this communication is strictly prohibited. If you have received this communication in error, please immediately notify us by telephone (if long distance, please call collect) and return the original message to us at the above address via the U.S. Postal Service. Thank you.
****

IF YOU DO NOT RECEIVE ALL PAGES OR IF YOU ENCOUNTER
ANY OTHER DIFFICULTY, PLEASE PHONE Erica
AT (408) 971-2573 AT YOUR EARLIEST CONVENIENCE

November 13, 2006

RECEIVED
CENTRAL FAX CENTER
NOV 13 2006

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	
McArdle et al.	Art Unit: 2135
Application No. 10/068,280	Examiner: Ha, Leynna A.
Filed: 02/04/2002	Date: 11/13/2006
For: INTRUSION PREVENTION FOR ACTIVE NETWORKED APPLICATIONS	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

REPLY BRIEF (37 C.F.R. § 41.37)

This Reply Brief is being filed within two (2) months of the mailing of the Examiner's Answer mailed on 09/11/2006.

Following is an issue-by-issue reply to the Examiner's Answer.

CERTIFICATE OF MAILING/TRANSMISSION (37 C.F.R. § 1.8(a))

I hereby certify that this correspondence is, on the date shown below, being:

MAILING

☐ deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to the Commissioner for Patents, Washington, D.C. 20231.

Date: 11/13/2006

FACSIMILE

☒ transmitted by facsimile to the Patent and Trademark Office, (571) 273-8300.

Signature

Erica L. Farlow

(type or print name of person certifying)

PAGE 2/34 * RCVD AT 11/13/2006 8:36:23 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):11-38

Issue # 1:

The Examiner has rejected Claim 51 under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The Examiner has specifically stated that appellant's claimed technique "wherein the heuristic rule includes information associated with an active networked application making a new connection never previously made" is not supported in the specification. Appellant respectfully points out page 5, lines 1-8 of the specification, which clearly states that "a heuristic rule may describe an attack that is based on unusual behavior, e.g. an application suddenly making a new, previously unseen connection" and that "[t]he system 100 applies a filter 103 based on the active networked applications." Thus, appellant's claim language is clearly supported by the specification.

In the Advisory Action mailed 03/15/2006, the Examiner argued that '[t]he proposed claim stated "a new connection never previously made" is interpreted as a brand new connection that never made or completed attempts before.' In addition, the Examiner argued that 'the specification states "a new, previously unseen connection", is not the same as a new connection "never" previously made.' Further, the Examiner argued that "[t]he claimed previously unseen connection of the specification is interpreted as a connection that was previously undetected or unknown of but does not mean a connection that was never made." Appellant respectfully disagrees with the Examiner's interpretation and respectfully asserts that page 5, lines 1-4 of the specification teaches that "a heuristic rule may describe an attack that is based on unusual behavior, e.g. an application suddenly making a new, previously unseen connection" (emphasis added). Appellant asserts that since the connection is new, it supports appellant's claimed "new connection never previously made," since a new connection would not previously have been seen.

In the Examiner's Answer mailed 09/11/2006, the Examiner stated that "[t]he rejection under 35 U.S.C. 112, 1st paragraph for claim 51 is withdrawn."

Issue # 2:

PAGE 3/34 * RCVD AT 11/13/2006 8:36:23 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):11-38

The Examiner has rejected Claims 1-12, 14-26, 28-40, 42-48, 50-51 under 35 U.S.C. 103(a) as being unpatentable over Freund (U.S. Patent No. 5,987,611) in view of Kaler et al. (U.S. Patent No. 6,671,829). Appellant respectfully disagrees with such rejection.

Group #1: Claims 1, 7-12, 14-15, 21-26, 28-29, 35-40, 42-43, 47, and 50

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

First element of prima facie case of obviousness: combining Freund and Kaler

With respect to the first element of the *prima facie* case of obviousness and, in particular, the obviousness of combining the aforementioned references, the Examiner argues that it would have been obvious to combine the teaching of the subset of intrusion rules in Freund with the teaching of filter reduction to extract only the information of interest as taught by Kaler because this reduces the performance impact of monitoring. To the contrary, appellant respectfully asserts that it would not have been obvious to combine the teachings of the Freund and Kaler references, especially in view of the vast evidence to the contrary.

For example, Freund relates to regulating access and maintaining security of individual computer systems and local area networks connected to larger open networks, while Kaler relates to analyzing the performance of a data processing system. To simply glean features from a security system, such as that of Freund, and combine the same with the *non-analogous art* of a performance analyzer, such as that of Kaler, would simply be improper. In particular, security systems actively protect computer systems, while performance analyzers merely collect data associated with a computer system for performance analysis. "In order to rely on a reference as a basis for rejection of an

PAGE 4/34 * RCVD AT 11/13/2006 8:36:23 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):11-38

[appellant's] invention, the reference must either be in the field of [appellant's] endeavor or, if not, then be reasonably pertinent to the particular problem with which the inventor was concerned." In re Oetiker, 977 F.2d 1443, 1446, 24 USPQ2d 1443, 1445 (Fed. Cir. 1992). See also In re Deminski, 796 F.2d 436, 230 USPQ 313 (Fed. Cir. 1986); In re Clay, 966 F.2d 656, 659, 23 USPQ2d 1058, 1060-61 (Fed. Cir. 1992). In view of the vastly different types of problems a security system addresses as opposed to a performance analyzer, the Examiner's proposed combination is inappropriate.

In the Advisory Action mailed 03/15/2006, the Examiner argued that "[t]he security system of Freund and performance analyzer of Kaler both monitors and filters data and therefore both comprises security prevention." In addition, the Examiner argues that "[t]o analyze the performance is clearly to attempt to protect the system, otherwise there is not a need to analyze its traffic or activities." However, the abstract of Kaler discloses "a distributed data processing system...[that] provide[s] a system user with tools for analyzing an application running thereon" in which "[i]nformation about the flow and performance of the application can be specified, captured, and analyzed, without modifying it or degrading its performance or data security characteristics, even if it is distributed across multiple machines" (Kaler, Abstract - emphasis added). Clearly, Kaler's disclosure that flow and performance information can be specified, captured, and analyzed, without degrading its data security characteristics *teaches away* from any sort of security system, contrary to the Examiner's assertion that Kaler "comprises security prevention." Thus, for the reasons argued above, the Examiner's proposed combination of Kaler's performance analyzer with Freund's security system is inappropriate.

In the Examiner's Answer mailed 09/11/2006, the Examiner has stated that "Freund teaches a system and method for client based monitoring and filtering (col. 3, lines 50-67)" and that "applications (software) can be a Web browser (i.e. Netscape Navigator or Microsoft Internet Explorer) which communicates with the Internet (col. 8, lines 2-10 and col. 15, lines 14-21)." Further, the Examiner has stated that "[a]n active application is where active use occurs when a user directly interacts with an Internet application while that application accesses the Internet (col. 10, lines 17-43)" and that the "client-based filter application performs all of the monitoring, logging , filter work, and also keeps a list of currently active processes and determines which process is actively used (col. 4, lines 31-37)." In addition, the Examiner has stated that "Freund discloses the

PAGE 5/34 * RCVD AT 11/13/2006 8:36:23 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):11-38

system can monitor TCP/IP activities on a per process or per application basis and it access rights (col. 4, lines 52-55)." Also, the Examiner has stated that "Freund discloses the set of intrusion rules are access rules for the entire LAN for one or more workgroups, or the specific user (col. 3, lines 61-63)" and that "[t]hese access rules include criteria in the form of subset of intrusion rules (col. 4, lines 9-27 and col. 5, lines 39-43) corresponding to the active networked application."

Further, in the Examiner's Answer mailed 09/11/2006, the Examiner has stated that "Kaler identifies a known problem with performance analysis for data processing systems is that very often such analysis provides opportunities for breaching the data security of such systems (col. 2, lines 64-67)" and "[t]hus, Kaler indicates there is a substantial need to provide automated tools for efficiently analyzing the performance, function and behavior of their applications without significantly affecting the performance or data security characteristics of the applications (col. 3, lines 39-45)." Additionally, the Examiner has stated that "Kaler includes filter(s) for event monitoring that is a way in which the system user can specify what is to be monitored in the system under examination (col. 22, lines 2-4)." Furthermore, the Examiner has stated that "Kaler discloses filtering a set of intrusion rules in the form of triggers that are set to monitor for a selected condition or error to occur (col. 21, lines 47-52)" and that "Kaler provides a secure environment for data collection through the use of discretionary access controls such that discretionary access controls may be based on authentication identities and encryption techniques (col. 22, line 53-col. 23, line 7)." Also, the Examiner states that "[h]ence, the subset of rules is from a process of filter reduction that extracts portions of a filter relevant to specify a specific portion of the monitoring infrastructure (col. 4, lines 56-61 and col. 23, lines 34-45)."

In addition, in the Examiner's Answer mailed 09/11/2006, the Examiner has stated that '[b]y reading further into the Kaler reference, appellant's points to "without modifying or degrading its data security characteristics" to show this teaches away from a security system.' The Examiner has argued that "this recitation is actually an advantage instead of a disadvantage to a security system because Kaler suggests that there is substantial need to provide automated tools for efficiently analyzing the performance, function and behavior of their applications without significantly affecting the performance or data security characteristics of the applications (col. 3, lines 39-45)" which "merely shows that Kaler's method will not affect the security or lower its standard for its data security characteristics and still maintain the flow and performance of the application."

PAGE 6/34 * RCVD AT 11/13/2006 8:36:23 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):11-38

Further, the Examiner argued that "[t]hus, without modifying or degrading its performance or data security characteristics teaches an added benefit to the security prevention" and "[t]herefore, Kaler's invention does have suggestions of security for the system (col. 21, lines 46-52 and col. 22, lines 45-55, and col. 23, lines 1-8)." In addition, the Examiner argues that "[t]hus, Kaler does not teach away from any sort of security system" and that 'Kaler is a proper secondary prior art in combination with Freund because the Freund and Kaler combination meets the first (element) basic criteria of "there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skills in the art to modify the references or to combine reference teachings."

Appellant respectfully disagrees with the Examiner's arguments and asserts that it would not have been obvious to combine Freund's security system with the *non-analogous art* of Kaler's performance analyzer, especially in view of the vast evidence to the contrary. The Examiner argued that "Kaler's method will not affect the security or lower its standard for its data security characteristics and still maintain the flow and performance of the application." However, appellant respectfully asserts that Kaler discloses that "IECs are only created for users who desire to monitor system performance" and that "[t]hey are automatically created when needed" (Kaler, Col. 13, lines 1-3). Further, Kaler discloses that "[t]his ensures that, if the system is not under analysis, the performance impact of operating the performance analyzer is negligible" and that "the system is able to remove all of the IECs from memory when analysis completes, so that a system wherein analysis has finished behaves with the same characteristics as before performance began, unlike many traditional tools" (Kaler, Col. 13, lines 3-10 – emphasis added). In addition, Freund is concerned with performance impacts and discloses that "[i]n a preferred embodiment, the data acquisition module 440 utilizes the shared message buffer 550, so that the module itself need not undertake various allocation/deallocation operations (which might degrade performance)" (Freund, Col. 21, lines 2-7). However, stating that the performance impact of operating the performance analyzer when the system is not under analysis implies that there is a performance impact when it is under analysis. Clearly, Kaler's performance analyzer *teaches away* from including the performance analyzer in the security system of Freund due to the performance impact during analysis.

Third element of prima facie case of obviousness

PAGE 7/34 * RCVD AT 11/13/2006 8:36:23 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):11-38

Appellant also respectfully asserts that the third element of the *prima facie* case of obviousness has also not been met by the references relied on by the Examiner.

Sub-Section 1 – the claimed "filtering a set of intrusion rules to create a subset of intrusion rules corresponding to the active networked application"

With respect to each of the independent claims, the Examiner has relied on the following excerpts from Freund to make a prior art showing of appellant's claimed "filtering a set of intrusion rules to create a subset of intrusion rules corresponding to the active networked application" (see the same or similar, but not necessarily identical language in each of the independent claims).

> "...the system can track files being created and changed by any process in order to match TCP/IP activities with corresponding file activities." (Col. 4, lines 65-67)
>
> "...which specifies rules which govern Internet access by the client computers including the particular client computer;
> c) Transmitting a filtered subset of the rules to the particular client computer." (Col. 5, lines 39-43)

Appellant respectfully asserts that the only rules in such excerpts relate to "rules which govern Internet access by the client computers." Clearly, rules that govern Internet access do not meet appellant's claimed "rules corresponding to the active networked application" (emphasis added).

Furthermore, simply because Freund teaches that a "system can track files created and changed by any process" does not inherently mean that there are rules corresponding to an active networked application, in the manner claimed by appellant.

Still yet, such excerpts do not even mention any sort of filtering, let alone "filtering a set of intrusion rules to create a subset of intrusion rules," as appellant specifically claims (emphasis added). In fact, appellant notes that the only subset of rules disclosed in Freund relate to "rules filtered for a given user" (see Claim 12 in Freund), and not to appellant's claimed "subset of intrusion rules corresponding to the active networked application" (emphasis added).

In the Advisory Action mailed 03/15/2006, in addressing appellant's claimed "filtering a set of intrusion rules to create a subset of intrusion rules," the Examiner argued that "Kaler was brought

PAGE 8/34 * RCVD AT 11/13/2006 8:36:23 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):11-38

forth to explain the filtering creating subset rules process" and "that a filter is a way in which a user can specify [what is] to be monitored in the system under examination (col. 22, lines 2-7)." However, a system user specifying what is monitored in a system fails to even suggest "filtering a set of intrusion rules to create a subset of intrusion rules corresponding to the active networked application" (emphasis added), as claimed by appellant.

Further, in the Advisory Action mailed 03/15/2006, in addressing appellant's claimed "filtering a set of intrusion rules to create a subset of intrusion rules corresponding to the active networked application," the Examiner argued that "Freund does have the claimed filtering rules corresponding to the active networked application (col. 10, lines 17-67)." Additionally, the Examiner argued that "Freund discusses monitoring and filtering work that is responsible for intercepting process loading and unloading (col. 4, lines 5-33 and col. 5, lines 55-62)."

After carefully reviewing the cited references, it is clear that Freund merely discloses that "[t]he client-based filter application, which in a preferred embodiment performs all of the monitoring, logging, and filtering work, is responsible for intercepting process loading and unloading" (emphasis added). Freund further discloses that the "Client Monitor compares application properties (version, executable name, and the like) with database of application allowed to access the Internet" (emphasis added). However, the client based filter application and the Client Monitor comparing application properties with a database of applications allowed to access the internet simply fails to meet "filtering a set of intrusion rules to create a subset of intrusion rules **corresponding to the active networked application**" (emphasis added), as claimed by appellant. The referenced excerpts from Freund simply fail to even suggest any rule filtering "corresponding to the active networked application," as claimed by appellant.

In the Examiner's Answer mailed 09/11/2006, under the heading of "**Page 12, 1st & 2nd paragraph of brief**," the Examiner has stated that "Freund discloses applications (software) can be a Web browser (i.e. Netscape Navigator or Microsoft Internet Explorer) which communicates through a communication layer or driver with the Internet (col. 8, lines 2-10 and col. 15, lines 14-21)." Further the Examiner has stated that "Freund discloses an active use occurs when a user directly interacts with an Internet Application while that application accesses the Internet (col. 10, lines 17-43)." In addition, the Examiner argued that "[r]ules can be interpreted as given permissions,

PAGE 9/34 * RCVD AT 11/13/2006 8:36:23 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):11-38

restrictions, or certain criteria for certain users, workstations, or applications such that rules are for regulating access or activity" and that "rules include criteria or subsets of rules (col. 5, lines 30-43) where the subset of rules includes a list of applications or application versions that a user can/cannot use, list of URLs that the application can/cannot use, or a list of protocols or protocol component an application can/cannot use (col. 4, lines 9-27)." Furthermore, the Examiner has argued that "[t]hese rules corresponds to the active networked application" and "[t]herefore, Freund teaches the claimed rules corresponding to the active networked application."

Appellant respectfully disagrees with the Examiner's arguments, particularly since the Examiner's assertions are not supported by what is actually disclosed by Freund. Specifically, appellant asserts that Freund merely discloses that "[t]he access management application is employed by the LAN administrator, workgroup administrator, and/or LAN user to maintain a database of the access rules for the workstations being administrated" where "[t]hese access rules can include criteria such as total time a user can be connected to the Internet (e.g., per day, week, month, or the like), time a user can interactively use the Internet (e.g., per day, week, month, or the like), a list of applications or application versions that a user can or cannot use in order to access the Internet..." (Col. 4, lines 5-14 – emphasis added). Further, Freund discloses that "[t]hese access rules can be qualified by optionally specifying: to whom should a rule apply (list of users, list of workgroups, or all)..." (Col. 4, lines 19-21 – emphasis added). In addition, Freund discloses "[i]nstalling at another computer on the local area network a supervisor process, which specifies rules which govern Internet access by the client computers including the particular client computer" and "[t]ransmitting a filtered subset of the rules to the particular client computer" (Col. 5, lines 37-42 – emphasis added). Freund further discloses that "[t]he supervisor monitors whether a client has the filter application loaded and provides the filter application with the rules for the specific user or workstation" (Col. 14, lines 2-5 – emphasis added).

By virtue of the above excerpts, appellant strongly asserts that Freund merely discloses maintaining a database of access rules for the workstations being administered where the access rules include criteria such as a list of applications a user can or cannot use, and that the access rules are qualified by whom the rule applies. Further, Freund discloses that a filtered subset of the rules specific to a user or workstation is transferred to the particular computer. However, Freund's disclosure that the filtering is performed based on the qualification on whom the rules apply (specific user or

PAGE 10/34 * RCVD AT 11/13/2006 8:36:23 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):11-38

workstation) simply fails to meet "filtering a set of intrusion rules to create a subset of intrusion rules corresponding to the active networked application" (emphasis added), as claimed by appellant. Clearly, the rules, as disclosed in Freund, are filtered based on the qualification to whom they apply (list of users, list of workgroups, or all). However, Freund does **not** disclose "filtering a set of intrusion rules to create a subset of intrusion rules corresponding to the active networked application" (emphasis added), as claimed by appellant.

In the Examiner's Answer mailed 09/11/2006, under the heading of "**Page 12, 3rd paragraph of brief**," the Examiner "traverses that Freund does not mention any sort of filtering" and has stated that "[t]he filtering application involves monitoring, logging, and filtering work (col. 3, lines 51-52 and col. 4, lines 29-32)" where "Freund discloses filtering as the ability to monitor and regulate Internet access on a per application basis by determining which applications can/cannot access the Internet (col. 4, lines 19-28 and col. 10, lines 55-65)." Additionally, the Examiner argued that "[f]iltering can be interpreted as sorting or looking for certain attributes or criteria" and "[r]ules regulates access such that rules can broadly be any permissions and restrictions or having specific attributes or criteria to indicate allowed access or unsafe."

Again, appellant respectfully disagrees with the Examiner's arguments and asserts that Freund merely discloses that "[t]he present invention provides system and methods for client-based monitoring and filtering of access" (Col. 3, lines 51-52 – emphasis added) and that "[t]he client-based filter application, which in a preferred embodiment performs all of the monitoring, logging, and filtering work, is responsible for intercepting process loading and unloading" (Col. 4, lines 29-32 – emphasis added). Freund further describes that "the filter application can determine if the process in question should have access to the Internet and what kind of access (i.e., protocols, Internet addresses, time limitations, and the like) is permissible for the given specific user" (Col. 13, lines 39-43 – emphasis added). Clearly, a client-based filter application that monitors and filters access to the Internet simply fails to suggest "filtering a set of intrusion rules to create a subset of intrusion rules **corresponding** to the active networked application" (emphasis added), as claimed by appellant.

Further, in the Examiner's Answer mailed 09/11/2006, under the heading of "**Page 12, 3rd paragraph of brief**," the Examiner has stated that "Freund discloses intrusion rules in the form of

PAGE 11/34 * RCVD AT 11/13/2006 8:36:23 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):11-38

access rules referring to one or more workgroups or users (col. 3, lines 62-63 and col. 4, lines 5-8)" where "[t]he access rules are specific to workstations/users that is allowed to have access to the Internet (col. 5, lines 10-12 and 23-41)" or that is used to block all clients that have not been verified (col. 4, lines 1-3)." In addition, the Examiner has stated that "Freund further discloses filtering the access rules sorts out the certain user/workstation allowed access or restricted access to the Internet to created filtered subset of rules (col. 5, lines 39-43 and col. 9, lines 4-13)" where "[t]hese subset of intrusion rules corresponds to the active networked applications because the rules pertain to applications that can/cannot access the Internet, protocols that the application can/cannot use (col. 4, lines 13-18) or applications with known security problems (col. 6, lines 1-3)." Furthermore, the Examiner has argued that "[t]hus, this obviously suggest filtering a set of intrusion rules creating a subset of intrusion rules." In addition, the Examiner has stated that "[t]he networked application is active when there are users/workstations interacting to the Internet using web browser (col. 6, lines 8-15 and col. 10, lines 18-20) and when the application is being monitored because the application is attempting to get access to the Internet (col. 10, lines 55-58)." Moreover, the Examiner has argued that "[t]hus, this obviously suggests active networked application and reads on the claimed filtering intrusion rules to create a subset of intrusion rules corresponding to the active networked application."

Again, appellant respectfully asserts that the Examiner has failed to consider the full weight of appellant's claims. Specifically, the Examiner has argued that "Freund further discloses filtering the access rules sorts out the certain user/workstation allowed access or restricted access to the Internet to created filtered subset of rules" (emphasis added). However, as argued hereinabove, appellant respectfully asserts that Freund discloses "[i]nstalling at another computer on the local area network a supervisor process, which specifies rules which govern Internet access by the client computers including the particular client computer" and "[t]ransmitting a filtered subset of the rules to the particular client computer" (Col. 5, lines 37-42 – emphasis added) where "[t]he supervisor monitors whether a client has the filter application loaded and provides the filter application with the rules for the specific user or workstation" (Col. 14, lines 2-5 – emphasis added). Clearly, the disclosure by Freund of providing a particular client computer a filtered set of rules specific to a user or workstation simply fails to even suggest "filtering a set of intrusion rules to create a subset of intrusion rules corresponding to the active networked application" (emphasis added), as claimed by appellant.

PAGE 12/34 * RCVD AT 11/13/2006 8:36:23 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):11-38

Additionally, in the Examiner's Answer mailed 09/11/2006, under the heading of "**Page 12, 3rd paragraph of brief**," the Examiner has stated that in "[a]nother example of filtering a set of intrusion rules to create a subset of rules corresponding to the active networked application," "Freund discloses comparing application properties (i.e. version, executable name) with the database of application allowed to access the Internet and checks what kind of activity (i.e. mail, browsing) the application is allowed to do (col. 5, lines 55-60)." Further, the Examiner has stated that "[t]he database obviously contain subset of intrusion rules since it is the application properties that is being compared to determine if the application is allowed access to the Internet or if violating any rules (col. 5, lines 46-52)." In addition, the Examiner has stated that "[t]he a set of intrusion rules is in the form of application properties such having the version type/number, executable name, and the like to allow access to the Internet." Further, the Examiner states that "[f]or instance, filtering the set of intrusion rules involves looking for the permitted application version type A to see if the specified attributes matches to the database of application allowed access to the Internet" where "[t]he filtering of application properties indicates the application version type A is allowed to access the internet which now creates the subset of rules for this version type A" and that "[t]he subset of rules indicates the kind of activity such as the application is allowed to browse (col. 5, lines 55-60)." Additionally, the Examiner has stated that "[a]nother example is comparing the application properties with the database of application with known security problems (col. 6, lines 1-3) where the certain version type or executable name has attributes of the database with application with known security problems is detected, then the subset of rules is to stop the application from accessing the Internet and/or warns the user (col. 6, lines 4-7)." Also, the Examiner has stated that "the networked application is active because Freund discloses the application attempts to access the Internet (col. 5, lines 55 and 67)."

Again, appellant respectfully disagrees with the Examiner's arguments and asserts that Freund merely discloses that when an "[a]pplication attempts to access [the] Internet," the "Client Monitor compares application properties (version, executable name, and the like) with [a] database of application allowed to access the Internet and checks what kind of activity the application is allowed to do (mail, browsing, and the like)," and "[i]f application is not allowed to access the Internet or not allowed to use the specific protocol then client monitor can stop application from accessing the Internet and/or warn user" (Col. 5, lines 54-64 – emphasis added). However, the mere disclosure

PAGE 13/34 * RCVD AT 11/13/2006 8:36:23 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):11-38

that application properties are used to check a database to determine if the activity is allowed for that application simply fails to suggest "filtering a set of intrusion rules to create a subset of intrusion rules corresponding to the active networked application" (emphasis added), as claimed by appellant. Further, since Freund discloses that the database used for the comparison contains multiple applications, and not just the active application, Freund fails to suggest "a subset of intrusion rules corresponding to the active networked application" (emphasis added), in the manner as claimed by appellant. Clearly, the result of the database lookup is to determine if the application is allowed access, and not to "create a subset of intrusion rules corresponding to the active networked application" (emphasis added), in the manner as claimed by appellant.

Furthermore, Freund illustrates that when an "[a]pplication attempts to access Internet", the "Client Monitor compares application properties (version, executable name, and the like) with [a] database of application with known security problems," and "[i]f [the] application has know[n] security problems, [the] client monitor stops the application from accessing the Internet and/or warns the user" (Col. 5, line 67-Col. 6, line 6 – emphasis added). Again, Freund's disclosure that the Client monitor uses application properties to check the database of applications to determine if the application may continue to use the Internet simply fails to suggest "filtering a set of intrusion rules to create a subset of intrusion rules corresponding to the active networked application" (emphasis added), as claimed by appellant.

In the Examiner's Answer mailed 09/11/2006, under the heading of "**Page 14 of brief**," the Examiner has stated that "[a]ppellant referencing col. 5, lines 46-59 and col. 8, lines 45-52 does not only relate to accessing the internet including rules associated with applications that are allowed to access the Internet." Further, the Examiner has stated that "Col. 5, lines 39-60 explains specifying rules which govern Internet access, transmitting a filtered subset of the rules to the particular client, and the process of determining whether the request to access the Internet would violate any rules." Furthermore, the Examiner has stated that "[t]his shows the filtering a set of intrusion rules to create the subset of intrusion rules corresponding to the active networked application."

Again, as argued hereinabove, appellant respectfully asserts that Freund's discloses "[i]nstalling at another computer on the local area network a supervisor process, which specifies rules which govern Internet access by the client computers including the particular client computer" and "[t]ransmitting

PAGE 14/34 * RCVD AT 11/13/2006 8:36:23 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):11-38

a filtered subset of the rules to the particular client computer" (Col. 5, lines 37-42 – emphasis added) where "[t]he supervisor monitors whether a client has the filter application loaded and provides the filter application with the rules for the specific user or workstation" (Col. 14, lines 2-5 – emphasis added). However, the disclosure by Freund of providing a computer a filtered set of rules specific to a user or workstation simply fails to even suggest "filtering a set of intrusion rules to create a subset of intrusion rules corresponding to the active networked application" (emphasis added), as claimed by appellant. Clearly, rules specific to a user or workstation simply fail to even suggest "subset of intrusion rules corresponding to the active networked application" (emphasis added), in the manner as claimed by appellant.

> *Sub-Section 2 - the claimed technique: "where the subset of the intrusion rules corresponding to the active networked application are capable of being used for evaluating intrusions that target the corresponding active networked application"*

Further, with respect to each of the independent claims, the Examiner has relied on the following excerpts from Freund to make a prior art showing of appellant's claimed technique "where the subset of the intrusion rules corresponding to the active networked application are capable of being used for evaluating intrusions that target the corresponding active networked application" (see the same or similar, but not necessarily identical language in each of the independent claims).

> "e) Determining whether the request for Internet access would violate any of the rules transmitted to the particular client computer, and
> f) If the request for Internet access violates any of the rules transmitted to the particular client computer, denying the request for Internet access.
> II. Using Application Properties to Determine Legitimate Internet Traffic
> a) Application attempts to access Internet;
> b) Client Monitor compares application properties (version, executable name, and the like) with database of application allowed to access the Internet and checks what kind of activity the application is allowed to do (mail, browsing, and the like)." (Col. 5, lines 46-59-emphasis added)

> "(1) The system should preferably be capable of restricting access to the Internet (or other Wide Area Network) to certain approved applications or/and application versions.
> (2) The system should preferably support centrally-maintained access rules (e.g., defining basic access rights), but at the same time allow individual workgroup managers or even individual users to set rules for their area of responsibility, if so desired by the organization." (Col. 8, lines 45-52)

PAGE 15/34 * RCVD AT 11/13/2006 8:36:23 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):11-38

Appellant respectfully asserts that such excerpts only relate to accessing the Internet, including rules associated with applications that are allowed to access the Internet (see emphasized excerpt above). Clearly, only teaching rules regarding accessing the Internet does not meet appellant's specific claim language, namely a "subset of the intrusion rules corresponding to the active networked application [that] are capable of being used for evaluating intrusions that target the corresponding **active networked application**" (emphasis added), as claimed.

In the Advisory Action mailed 03/15/2006, in addressing appellant's claimed "subset of the intrusion rules corresponding to the active networked application," the Examiner argued that "[t]he claimed set of intrusion rules is merely interpreted as more than one intrusion rules where Freund does teach more than one intrusion rules and subset rules for the client computer (col. 5, lines 35-62)." Specifically, Freund discloses "[i]nstalling ... a supervisor process, which specifies rules which govern Internet access by the client computers including the particular client computer" and "[t]ransmitting a filtered subset of the rules to the particular client computer" (emphasis added). However, merely specifying rules governing Internet access and transmitting a filtered subset of access rules fails to disclose a technique "where the subset of the **intrusion** rules corresponding to the active networked application are capable of being used for evaluating intrusions that target the corresponding active networked application" (emphasis added), as claimed by appellant.

Further, in the Advisory Action mailed 03/15/2006, in addressing appellant's claimed "subset of the intrusion rules ... [which] are capable of being used for evaluating intrusions that target the corresponding active networked application," the Examiner argued that "[m]onitoring the application of the computer being used is to access the internet where there involves rules and subset rules to regulate access on a per application basis (col. 10)." The Examiner continued, arguing that "[t]hese filtering rules and subset rules, which includes monitoring a given active application, total time particular applications access the Internet, and limiting the number of (approved) applications are secure measures for evaluating the active networked applications for intrusions."

Appellant respectively asserts that such excerpts from Freund merely teach that '[a] given application itself can be examined for determining whether it is "active" by determining whether the application receives "focus" and/or receives user input' (Col. 10, lines 40-43). In addition, Freund teaches that "the Internet access monitoring system of the present invention can track Internet access

PAGE 16/34 * RCVD AT 11/13/2006 8:36:23 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):11-38

on a per application basis--that is, access broken down by the application or applications used for the access" (Col. 10, lines 47-50). However, monitoring the total time the user is browsing the Internet with an application that has the user focus simply fails to meet a technique "where the subset of the intrusion rules corresponding to the active networked application are capable of being used for **evaluating intrusions** that target the corresponding active networked application" (emphasis added), as claimed by appellant. Appellant asserts that merely disclosing rules for monitoring user Internet usage fails to meet a subset of rules "for evaluating intrusions that target the corresponding active networked application" (emphasis added), as claimed by appellant.

In the Examiner's Answer mailed 09/11/2006, under the heading of "**Page 13 of brief**," the Examiner has stated that "Freund discloses the subset of intrusion rules (i.e. mail, browsing, or stop from accessing the internet and warns user) are stored in the databases are compared to when application attempts to access Internet (col. 5, lines 55 – col. 6, line 15)." Furthermore, the Examiner has stated that "[t]hus, the subset of intrusion rules can be used for evaluating intrusions that target the corresponding active networked application against the database of applications with known security problems (col. 6, lines 1-3)." In addition, the Examiner has stated that "[t]he application is active because it is attempting to access the Internet (col. 6, lines 4-7)" and "[t]herefore, this reads on subset of the intrusion rules corresponding to the active networked application are capable of being used for evaluating intrusion that target the corresponding active networked application (col. 5, lines 45-51 and col. 6, lines 5-15)."

Appellant respectfully disagrees with the Examiner's arguments and asserts that Freund merely discloses that "[t]hese access rules can include criteria such as ... a list of applications or application versions that a user can or cannot use in order to access the Internet, a list of URLs (or WAN addresses) that a user application can (or cannot) access, a list of protocols or protocol components (such as Java Script™) that a user application can or cannot use" (Col. 4, lines 8-17 – emphasis added). Further, Freund discloses that "Client Monitor compares application properties (version, executable name, and the like) with database of application allowed to access the Internet and checks what kind of activity the application is allowed to do (mail, browsing, and the like)" (Col. 5, lines 55-60). In addition, Freund discloses that "Client Monitor compares application properties (version, executable name, and the like) with database of application with known security problems" and "[i]f application has know security problems, client monitor stops the application from

PAGE 17/34 * RCVD AT 11/13/2006 8:36:23 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):11-38

accessing the Internet and/or warns the user" (Col. 6, lines 1-6 – emphasis added). Furthermore, Freund discloses "[d]etermining whether the request for Internet access would violate any of the rules transmitted to the particular client computer" and "[i]f the request for Internet access violates any of the rules transmitted to the particular client computer, denying the request for Internet access" (Col. 5, lines 46-52 – emphasis added).

However, the mere disclosure by Freund that access rules include criteria such as a list of applications that a user can or cannot use, a list of URLs that a user application can or cannot access, and list of protocols that a user application can or cannot use fails to even suggest a technique "where the subset of the intrusion rules corresponding to the active networked application are capable of being used for evaluating intrusions that target the corresponding active networked application" (emphasis added), as claimed by appellant. In addition, denying the request for Internet access if the request violates an of the rules, as in Freund, fails to suggest "the subset of the intrusion rules ... being used for evaluating intrusions that target the corresponding active networked application" (emphasis added), in the manner as claimed by appellant. Furthermore, disclosing that the Client Monitor compares application properties against a database fails to suggest "**evaluating intrusions** that **target** the corresponding active networked application" (emphasis added), in the manner as claimed by appellant.

In the Examiner's Answer mailed 09/11/2006, under the heading of "**Page 15 of brief**," the Examiner has stated that "Col. 10, lines 18-50 explains the networked application is active by the interaction of a user" and that "Freund also discloses the application as being monitored is active because the application is attempting to access the Internet." Further, the Examiner has stated that "Freund discloses the evaluating intrusions of an active networked application with the ability to monitor and regulate Internet access by specifying which applications can or cannot access the Internet (col. 10, lines 55-58)" and that "Freund further explains the monitoring access to the Internet by individual applications allowing the system to not only track Internet traffic but determine data exchanged on a per application basis including the ability to determine the name of individual files downloaded." Additionally, the Examiner has stated that "[t]he approach creates an audit trail of downloaded files thus allowing one to trace the source of files found to contain offensive contents or pose security risks (col. 11, lines 1-18)." Also, the Examiner has stated that "[a]nother form of evaluating intrusions is where Freund discloses the subset of intrusion rules (i.e.

PAGE 18/34 * RCVD AT 11/13/2006 8:36:23 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):11-38

mail, browsing, or stop from accessing the internet and warns user) are stored in the databases are compared to when application attempts to access Internet (col. 5, lines 55 – col. 6, line 15)" and "[t]hus, the subset of intrusion rules can be used for evaluating intrusions that target the corresponding active networked application against the database of applications with known security problems (col. 6, lines 1-3)." Furthermore, the Examiner has stated that "[t]he application is active because it is attempting to access the Internet (col. 6, lines 4-7)" and "[t]herefore, this reads on subset of intrusion rules corresponding to the active networked application are capable of being used for evaluating intrusion that target the corresponding active networked application (col. 5, lines 45-51 and col. 6, lines 5-15)."

Appellant respectfully disagrees with the Examiner's arguments and asserts that Freund merely discloses that "Client Monitor compares application properties (version, executable name, and the like) with database of application allowed to access the Internet and checks what kind of activity the application is allowed to do (mail, browsing, and the like)" (Col. 5, lines 55-60). Further, Freund discloses that "Client Monitor compares application properties (version, executable name, and the like) with database of application with known security problems" and "[i]f application has know security problems, client monitor stops the application from accessing the Internet and/or warns the user" (Col. 6, lines 1-6 – emphasis added). In addition, Freund discloses "[d]etermining whether the request for Internet access would violate any of the rules transmitted to the particular client computer" and "[i]f the request for Internet access violates any of the rules transmitted to the particular client computer, denying the request for Internet access" (Col. 5, lines 46-52 – emphasis added). Also, Freund discloses that "[t]he ability to monitor and regulate Internet access on a per application basis is particularly advantageous" where the "[a]dvantages include, for instance, the ability to specify which applications can (and cannot) access the Internet" (Col. 10, lines 55-58 – emphasis added).

However, the mere disclosure by Freund that the Client Monitor compares application properties to a database of applications allowed to access the Internet to check for the kind of allowed activity, and that Client Monitor compares application properties to a database of applications with known security problems to stop the applications with known security problems from accessing the Internet fails to suggest a technique "where the subset of the intrusion rules corresponding to the active networked application are capable of being used for **evaluating intrusions** that **target** the

PAGE 19/34 * RCVD AT 11/13/2006 8:36:23 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):11-38

corresponding active networked application" (emphasis added), as claimed by appellant. Clearly, checking a database to determine if an application is allowed to access the Internet fails to suggest "**evaluating intrusions** that **target** the corresponding active networked application" (emphasis added), in the manner as claimed by appellant. Moreover, Freund's disclosure of denying Internet access if the request violates the transmitted rules fails to suggest "**evaluating intrusions** that **target** the corresponding active networked application" (emphasis added), in the manner as claimed by appellant.

Appellant strongly asserts that Freund's disclosure of checking databases for application properties, and Internet access rules clearly fail to even suggest a technique "where the subset of the intrusion rules corresponding to the active networked application are capable of being used for **evaluating intrusions** that **target** the corresponding active networked application" (emphasis added), as claimed by appellant.

> *Sub-Section 3 - the claimed technique "wherein the subset of the intrusion rules corresponding to the active networked application are used for the evaluation for reducing a required amount of processing resources"*

Still yet, with respect to each of the independent claims, the Examiner has relied on the following excerpts et al. from Freund and Kaler to make a prior art showing of appellant's claimed technique "wherein the subset of the intrusion rules corresponding to the active networked application are used for the evaluation for reducing a required amount of processing resources."

> "If a process uses FTP to download a file, for example, the system will match that activity to a file being saved by the same process by checking file name and size. If a match is found, a log entry is generated. This allows the immediate application of internal or external virus checkers." (Freund: Col. 13, lines 59-65)
>
> "Filter reduction is used to narrow the scope of the filter to extract only the information of interest and hence reduce the performance impact of monitoring." (Kaler: Col. 4, lines 57-61)

First, appellant respectfully asserts that the excerpt in Freund relied on by the Examiner does not even suggest any sort of "subset of the intrusion rules," as the Examiner contends (emphasis added), but instead only teaches matching activity to a file. Thus, since Freund does not disclose a subset in

PAGE 20/34 * RCVD AT 11/13/2006 8:36:23 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):11-38

the context claimed by appellant, Freund cannot teach, even in combination with Kaler, a subset that is "used for the evaluation for reducing a required amount of processing resources." Furthermore, appellant notes that, when read in context, Kaler's filter reduction only relates to a user that specifies which items to filter such that events are collected only for the specified items (see Kaler, Col. 37, line 47- Col. 38, line 5). Thus, Kaler does not teach a subset of intrusion rules, as claimed by appellant, but instead only teaches a filter that collects events for specified items.

In the Examiner's Answer mailed 09/11/2006, under the heading of "**Page 12, 4th & 5th paragraph of brief**," the Examiner has stated that "[t]he Advisory Action (3/15/2006) briefly discusses the Kaler reference" and "[t]hus, the Final Office Action (11/15/2005) better explains the Freund and Kaler combination." Further, the Examiner has stated that "Freund discloses filtering creating the subset of intrusion rules corresponding to the active networked application but fails to further explain details of the subset of intrusion rules are used for reducing a required amount of processing resources" and "[t]hus, Kaler is brought forth to teach this limitation." In addition, the Examiner has stated that "[a]s discussed previously, Freund is the primary reference brought forth disclosing the claimed filtering (col. 4, lines 29-32 and col. 10, lines 55-65) a set of intrusion rules (col. 3, lines 61-63 and col. 4, lines 1-3) to create a subset of intrusion rules (col. 4, lines 5-27 and col. 6, lines 1-3) corresponding to the active networked application (col. 10, lines 17-43)." Additionally, the Examiner has stated that '[i]n the Advisory Action (3/15/2006), states that Freund does have the claimed "filtering rules",' '[h]owever, the examiner meant subset rules corresponding to the active networked application because the claimed invention does not recite "filtering rules corresponding to the active networked application"' and only "recites filtering a set of intrusion rules to create the subset of intrusion rules corresponding to the active networked application." Moreover, the Examiner has stated that "[t]hus, the set of intrusion rules have not limited to applications, users, or workstations whereas the subset of intrusion rules limits to only applications," and "[a]s such, Freund's intrusion rules may apply to the user/workstation (col. 3, lines 61-65 and col. 5, lines 30-60)." Further, the Examiner has stated that "[t]he user/workstation have access to certain applications where those applications have certain access (subset of intrusion rules) to access the Internet (col. 4, lines 5-27)."

In addition, the Examiner has stated that "Freund discloses intrusion rules is in the form of access rules refers to one or more workgroups or users (col. 3, lines 62-63 and col. 4, lines 5-8)" where

PAGE 21/34 * RCVD AT 11/13/2006 8:36:23 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):11-38

"[t]he access rules are specific to workstations/users that are allowed to have access to the Internet (col. 5, lines 10-12 and 23-41) or to block all clients that have not been verified (col. 4, lines 1-3)." The Examiner has stated that "Freund further discloses filtering the access rules sorts out the certain user/workstation allowed access or restricted access to the Internet to create filtered subset of rules (col. 5, lines 39-43 and col. 9, lines 4-13)" where "[t]hese subset of intrusion rules corresponds to the active networked applications because the rules pertains to applications that can/cannot access the Internet, protocols that the application can/cannot use (col. 4, lines 13-18) or applications with known security problems (col. 6, lines 1-3)." The Examiner has stated "[t]hus, this obviously suggests filtering a set of intrusion rules creating subset of intrusion rules." Further, the Examiner has stated that "[t]he networked application is active when there are users/workstations interacting to the Internet using web browser (col. 6, lines 8-15 and col. 10, lines 18-20) and when the application is being monitored because the application is attempting to get access to the Internet" (col. 10, lines 55-58). The Examiner has stated "[t]hus, this obviously suggest active networked application and reads on the claimed filtering intrusion rules to create a subset of intrusion rules corresponding to the active networked application." In addition, the Examiner has stated that "Freund discloses the subset of intrusion rules corresponding to the active networked application but fails to further explain details of the subset of intrusion rules are used for reducing a required amount of processing resources" and that "[i]t is obvious the subset of intrusion rules is reduced or narrowed down to certain criteria for evaluation corresponding to the active networked application."

Most pointedly, the Examiner has concluded "[h]ence, Kaler teaches filter reduction is used to narrow the scope of the filter to extract only the information of interest and hence reduce the performance impact of monitoring results the subset of intrusion rules (col. 4, lines 55-61 and col. 23, lines 34-45)."

Appellant respectfully disagrees with the Examiner's arguments and asserts Freund fails to meet appellant's claimed technique "wherein the subset of the intrusion rules corresponding to the active networked application," in the manner as claimed, for the reasons argued hereinabove. Further, appellant respectfully disagrees with the Examiner's arguments that Col. 4, lines 55-61, and Col. 23, lines 33-45 of Kaler meets appellant's claimed "subset of the intrusion rules ... used for the evaluation for reducing a required amount of processing resources," as claimed by appellant. Appellant respectfully asserts that Kaler merely discloses that "[f]ilter reduction is used to narrow

PAGE 22/34 * RCVD AT 11/13/2006 8:36:23 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):11-38

the scope of the filter to extract only the information of interest and hence reduce the performance impact of monitoring" (Col. 4, lines 56-61 – emphasis added). Freund further discloses that "[f]ilter reduction is a process employed by the VSA to extract portions of a filter relevant to specify a specific portion of the monitoring infrastructure" (Col. 23, lines 34-37 – emphasis added).

However, the mere disclosure of Kaler that filter reduction narrows the scope of the filter to extract only information of interest, or a relevant portion of the filter, in order to reduce the performance impact of monitoring simply fails to even suggest a technique "wherein the subset of the intrusion rules corresponding to the active networked application are used for the evaluation for reducing a required amount of processing resources" (emphasis added), as claimed by appellant. Clearly, reducing a filter for monitoring fails to suggest that "the subset of the intrusion rules ... are used for the evaluation" (emphasis added), in the manner as claimed by appellant.

In view of the above, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met.

Group #2: Claims 2, 16, 30, and 44

With respect to Claim 2 et al., the Examiner has relied on Col. 4, lines 51-62 in Freund to make a prior art showing of appellant's claimed "detecting when the active networked application becomes inactive; and re-filtering the set of intrusion rules."

Appellant respectfully asserts that the only mention of an application in such excerpt merely relates to a "system [that] can monitor TCP/IP activities on a...per application basis." Freund simply fails to even suggest a situation where an "active networked application becomes inactive" (emphasis added), and especially does not teach that, when such occurs, "the set of intrusion rules [are re-filtered]," as claimed by appellant.

In the Examiner's Answer mailed 09/11/2006, the Examiner has stated that "Freund discloses detecting when the active networked application becomes inactive is when there are violated rules for the attempt to access the Internet because the communication is terminated or stops the application from accessing the Internet (col. 4, lines 59-61 and col. 5, lines 60-63)." Further, the

PAGE 23/34 * RCVD AT 11/13/2006 8:36:23 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):11-38

Examiner has argued that "its is obvious that if the application is terminated from communicating or access the Internet is when the application becomes inactive" and "Freund also discusses re-filtering by redirecting the access after the violated rules occurred (col. 4, lines 27-28)."

Appellant respectfully disagrees with the Examiner's arguments and asserts that Freund merely discloses "what should happen if a rule is violated (e.g., denying Internet access, issuing a warning, redirecting the access, creating a log entry, or the like)" (Col. 4, lines 27-28 – emphasis added). Further, Freund discloses that "the prescribed remedial action for any violated rule is performed, including logging an exception log entry, and depending on the rules the TCP/IP activity, the communication is either terminated, redirected, modified, or continued" (Col. 4, lines 58-62 – emphasis added). In addition, Freund discloses that "[i]f application is not allowed to access the Internet or not allowed to use the specific protocol then client monitor can stop application from accessing the Internet and/or warn user" (Col. 5, lines 61-64 – emphasis added).

However, the mere disclosure by Freund that the Internet access is denied or the communication is terminated when a rule is violated, and that if an application is not allowed, then the client monitor stops the application from accessing the Internet simply fails to even suggest "detecting when the active networked application becomes inactive; and re-filtering the set of intrusion rules" (emphasis added), as claimed by appellant. Clearly, stopping a client from accessing the Internet, as disclosed by Freund, fails to meet "detecting when the active networked application becomes inactive" (emphasis added), in the manner as claimed by appellant. Further, the mere disclosure of redirecting the access when a rule is violated fails to suggest "re-filtering the set of intrusion rules" (emphasis added), in the manner as claimed by appellant.

In view of the above, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met.

Group #3: Claims 3, 4, 17, 18, 31, and 32

With respect to Claims 3 and 4 et al., the Examiner has relied on Col. 13, lines 20-22 in Freund to make a prior art showing of appellant's claimed technique "wherein the detecting comprises:

PAGE 24/34 * RCVD AT 11/13/2006 8:36:23 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):11-38

monitoring network connection terminations" (Claim 3 et al.) and "wherein the detecting comprises: monitoring application terminations" (Claim 4 et al.).

Appellant respectfully asserts that such excerpt from Freund only discloses that "if a rule is violated...[then] Internet access [is denied]." Clearly, denying internet access in the case that a rule is violated does not even suggest any sort of monitoring, let alone specifically "monitoring network connection terminations" and/or "monitoring application terminations," as claimed by appellant.

In the Examiner's Answer mailed 09/11/2006, the Examiner has stated that "Freund discloses tracking Internet activity and the ability to monitor and regulate access for applications that includes specifying which applications can or cannot access the internet (col. 10, lines 45-58)" and "when an application attempting to access the Internet and violated rules, the application is denied access and stops the application from accessing the Internet (col. 5, lines 61-64)." Further, the Examiner has argued that "[t]hus, it's obvious that Freund monitors both when access is allowed and connection termination once the application is stopped from accessing the Internet."

Appellant respectfully disagrees with the Examiner's arguments and asserts that Freund merely discloses "the prescribed remedial action for any violated rule is performed, including logging an exception log entry and, depending on the rules the TCP/IP activity, the communication is either terminated, redirected, modified, or continued" (Col. 13, lines 51-55). Further, Freund discloses that "[t]he ability to monitor and regulate Internet access on a per application basis is particularly advantageous" where such "[a]dvantages include, for instance, the ability to specify which applications can (and cannot) access the Internet" (Col. 10, lines 55-58). In addition, Freund discloses "[i]f application is not allowed to access the Internet or not allowed to use the specific protocol then client monitor can stop application from accessing the Internet and/or warn user" (Col. 5, lines 61-64).

However, the mere disclosure that prescribed remedial action for any violated rule includes terminating the communication, and that the client monitor may stop the application from accessing the Internet simply fails to even suggest appellant's claimed techniques "wherein the detecting comprises: monitoring network connection terminations" (Claim 3 et al.) and "wherein the detecting comprises: monitoring application terminations" (Claim 4 et al.), as claimed by appellant. Clearly,

PAGE 25/34 * RCVD AT 11/13/2006 8:36:23 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):11-38

an action including terminating the communication fails to meet "monitoring network connection terminations" or "monitoring application terminations," in the manner as claimed by appellant. Further, the mere disclosure of monitoring and regulating Internet access on a per application basis fails to suggest appellant's claimed "monitoring network connection terminations," or "monitoring application terminations," in the manner as claimed by appellant.

Again, in view of the above, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met.

Group #4: Claims 5, 6, 19, 20, 33, 34, 45, and 46

With respect to Claim 5 et al., the Examiner has relied on Col. 13, lines 50-56 and Col. 26, lines 55-58 in Freund to make a prior art showing of appellant's claimed "detecting when no networked application is active; and suspending the evaluating of network traffic until a networked application is active."

Appellant respectfully asserts that such excerpts only relate to "prescribed remedial action for any violated rule" such that "the communication is...terminated." Clearly, terminating a communication upon detection of a rule violation, as in Freud, does not even remotely relate to appellant's claim language, namely "detecting when no networked application is active," let alone where "the evaluating of network traffic [is suspended] until a networked application is active" (emphasis added).

In the Examiner's Answer mailed 09/11/2006, the Examiner has stated that "[t]he Freund and Kaler combination did not include detecting when no networked application is active, and suspending the evaluating of network traffic until a networked application is active." However, the Examiner has rejected Claims 5, 6, 19, 20, 33, 34, 45, and 46 under 35 U.S.C. 103(a) as being unpatentable over Freund and Kaler, in further view of Hanko et al. (U.S. Patent No. 6,912,578). Appellant respectfully disagrees with the new grounds of rejection.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally

PAGE 26/34 * RCVD AT 11/13/2006 8:36:23 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):11-38

available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck,*947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

First element of prima facie case of obviousness: combining Freund and Kaler, with Hanko

With respect to the first element of the prima facie case of obviousness and, in particular, the obviousness of combining the aforementioned references, the Examiner argues that it would have been obvious "to combine the teaching and monitoring and filtering with intrusion rules of the Freund and Kaler with the teaching of causing the application to stop consuming resources when detecting an application is inactive and to restart when the application active (col. 3, lines 45-52) because this improves resource utilization (col. 4, lines 16-17)." To the contrary, appellant respectfully asserts that it would not have been obvious to combine the teachings of the Hanko reference with the teachings of the Freund and Kaler references, especially in view of the vast evidence to the contrary.

For example, Freund relates to a security system, while Hanko relates to improving resource utilization on a shared client. To simply glean features from a security system, such as that of Freund, and combine the same with the *non-analogous art* of improving utilization on a shared client system, such as that of Hanko, would simply be improper. In particular, the security system of Freund utilizes a "client-based filter and [a] centralized supervisor application" (Freund, Col. 5, lines 16-17), while improving utilization on a shared client system utilizes a "thin-client architecture [where] the functionality of the end user computer is reduced to the point that, for the most part, only input and output capabilities exist" (Hanko, Col. 1, lines 18-20). "In order to rely on a reference as a basis for rejection of an [appellant's] invention, the reference must either be in the field of [appellant's] endeavor or, if not, then be reasonably pertinent to the particular problem with which the inventor was concerned." In re Oetiker, 977 F.2d 1443, 1446, 24 USPQ2d 1443, 1445 (Fed. Cir. 1992). See also In re Deminski, 796 F.2d 436, 230 USPQ 313 (Fed. Cir. 1986); In re Clay, 966 F.2d 656, 659, 23 USPQ2d 1058, 1060-61 (Fed. Cir. 1992). In view of the vastly

PAGE 27/34 * RCVD AT 11/13/2006 8:36:23 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):11-38

different types of problems a security system addresses as opposed to improving utilization on a shared client system, the Examiner's proposed combination is inappropriate.

Further, Kaler relates to analyzing the performance of a data processing system, while Hanko relates to improving resource utilization on a shared client. To simply glean features from a performance analyzer, such as that of Kaler, and combine the same with the *non-analogous art* of improving utilization on a shared client system, such as that of Hanko, would simply be improper. In particular, the security system of Kaler utilizes a "distributed data processing system" (Kaler, Abstract), while improving utilization on a shared client system utilizes a "thin-client architecture [where] the functionality of the end user computer is reduced to the point that, for the most part, only input and output capabilities exist" (Hanko, Col. 1, lines 18-20). "In order to rely on a reference as a basis for rejection of an [appellant's] invention, the reference must either be in the field of [appellant's] endeavor or, if not, then be reasonably pertinent to the particular problem with which the inventor was concerned." In re Oetiker, 977 F.2d 1443, 1446, 24 USPQ2d 1443, 1445 (Fed. Cir. 1992). See also In re Deminski, 796 F.2d 436, 230 USPQ 313 (Fed. Cir. 1986); In re Clay, 966 F.2d 656, 659, 23 USPQ2d 1058, 1060-61 (Fed. Cir. 1992). In view of the vastly different types of problems a performance analyzer addresses as opposed to improving utilization on a shared client system, the Examiner's proposed combination is inappropriate.

Third Element of Prima Facie case of obviousness

Appellant also respectfully asserts that the third element of the *prima facie* case of obviousness has also not been met by the references relied on by the Examiner. Specifically, the Examiner has argued that "Hanko discloses using traditional computer programs on a shared client by monitoring the status of an application, determining when an application no longer needs resources and causing the application to stop consuming resources (col. 3, lines 34-37)." Further, the Examiner has argued that "[t]he invention has a mechanism to stop a program from consuming resources when it detects a user has stopped interaction with an application and to restart it when the user begins interaction with it (col. 5, lines 21-28)" and "[w]hen there is no interaction regarding the application, it becomes inactive (col. 5, lines 10-13)." In addition, the Examiner has argued that "[t]his inactive application no longer consumes resources and is not being evaluated or suspended for the time being until the application returns to its original (active) state again (col. 12, lines 33-45 and 55-62)."

PAGE 28/34 * RCVD AT 11/13/2006 8:36:23 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):11-38

Appellant respectfully disagrees with the Examiner's arguments and asserts that Hanko merely discloses "monitoring the status of an application, determining when an application no longer needs resources, and causing the application to stop consuming resources" (Col. 3, lines 34-37). Further, Hanko discloses that "[w]hen the user interaction stops, the invention has a mechanism to stop a program from consuming resources (or to reduce its resource usage) and to restart it (or return it to its original state) later..." (Col. 5, lines 21-28 – emphasis added). In addition, Hanko discloses "[t]he invention determines when a user will not interact with an application 700" and "[w]hen it does it transmits a STOP signal 701 to one or more applications within the session to halt the consumption of resources while there is no chance of user input and no need for user output" (Col. 12, lines 33-37 – emphasis added). Also, Hanko discloses that "when the user later connects to the same or a different DTU, a CONTINUE signal (or message) is sent to each application process that was sent a STOP signal (or message) when the session was disconnected" (Col. 12, 55-62).

However, the mere disclosure of stopping a program when user interaction stops, when there is no chance of user input, and no need for user output simply fails to even suggest "detecting when no networked application is active; and suspending the evaluating of network traffic until a networked application is active" (emphasis added), as claimed by appellant. Clearly, the mere disclose of no user interaction fails to suggest "when no networked application is active" (emphasis added), in the manner as claimed by appellant. Further, halting the resources of an application where the user has stopped interaction, clearly fails to even suggest "suspending the evaluating of network traffic until a networked application is active" (emphasis added), in the manner as claimed by appellant.

In view of the above, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met.

Group #5: Claim 48

With respect to Claim 48, the Examiner has relied on Col. 11, line 56-Col. 12, line 17 and Col. 13, lines 13-22 in Freund to make a prior art showing of appellant's claimed technique "wherein the intrusion rules include information selected from the group consisting of a targeted active networked application, a specific hostile payload, a network port, and a protocol."

PAGE 29/34 * RCVD AT 11/13/2006 8:36:23 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):11-38

Appellant respectfully asserts that Col. 11, line 56-Col. 12, line 17 does not relate to intrusion rules, as claimed by appellant, but instead only relates to the protocol the Internet uses. In addition, Col. 13, lines 13-22 only discloses that the rules can specify "to whom the rule should apply...start date and expiration date of a rule; time of day when the rules should be applied...whether the rule is 'disclosed' to the user or workgroup...whether a rule ca be overwritten...and what should happen if a rule is violated." Clearly, such information associated with the rules as taught in Freund only relate to the application of the rules, and not to the substance of the rules including "a targeted active networked application, a specific hostile payload, a network port, and a protocol," as specifically claimed by appellant.

In the Examiner's Answer mailed 09/11/2006, the Examiner has argued that "Freund discloses monitoring access to the Internet by individual applications allows the system to not only track Internet traffic but also can determine data exchanged on a per application basis including the ability to determine the name of individual files downloaded as well as target directories to where such files are copied." The Examiner continued, stating that "[t]his approach creates an audit trail of downloaded files thus allowing one to trace the source file found to contain offensive contents or pose security risks (col. 11, lines 9-18)." Further, the Examiner has argued that "Freund includes access rules in the monitoring and filtering invention to determine what the user/workstation and the application can or cannot access" where "[t]he cannot access is considered to intrusion of Freund's access rules." In addition, the Examiner has argued that "[t]he can or cannot access rules includes a list of protocols or protocol components and list of applications or application versions (col. 4, lines 13-18)." Also, the Examiner has argued that "Freund further include displaying a selection of actions to undertake in the event that a rule is violated (col. 26, lines 45-65)" and that "examples are denying Internet access or issue a warning (col. 4, lines 26-28)."

Appellant respectfully disagrees with the Examiner's arguments and asserts that Freund discloses that "[t]hese access rules can include criteria such as ... a list of applications or application versions that a user can or cannot use in order to access the Internet, a list of URLs (or WAN addresses) that a user application can (or cannot) access, a list of protocols or protocol components (such as Java Script™) that a user application can or cannot use" (Col. 4, lines 8-17 – emphasis added) and "what should happen if a rule is violated (e.g., denying Internet access, issue a warning, redirecting the

PAGE 30/34 * RCVD AT 11/13/2006 8:36:23 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):11-38

access, creating a log entry, or the like)" (Col. 4, lines 26-28 – emphasis added). Further, Freund discloses that "monitoring access to the Internet by individual applications" (Col. 11, lines 9-18) and that "the rule disallows Internet access for all applications except Internet Explorer™ and Netscape Navigator™ browser software for all users and computers except for the marketing group, the Web server computer, and one individual" (Col. 26, lines 45-65).

However, the mere disclosure that the access rules include criteria such as a list of applications that a user can or cannot use, and a list of protocols that a user application can or cannot not use simply fails to even suggest a technique "wherein the intrusion rules include information selected from the group consisting of a targeted active networked application, a specific hostile payload, a network port, and a protocol" (emphasis added), as claimed by appellant. Further, Freund's disclosure of monitoring an individual application's access to the Internet and disallowing Internet access for all applications except Internet Explorer™ and Netscape Navigator™ fails to suggest a technique "wherein the intrusion rules include information selected from the group consisting of a targeted active networked application, a specific hostile payload, a network port, and a protocol" (emphasis added), as claimed by appellant. Clearly, a list of protocols that a user application can or cannot use to access the Internet fails to even suggest "a protocol," in the manner as claimed by appellant. Further, a list of applications that a user can or cannot to access the Internet simply fails to suggest a "targeted active networked application" (emphasis added), in the manner as claimed by appellant.

Again, in view of the above, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met.

Group #6: Claim 51

With respect to Claim 51, the Examiner has relied on Col. 10, lines 31-44; Col. 30, lines 13-15; Col. 13, lines 34-42; and Col. 5, lines 39-43 in Freund to make a prior art showing of appellant's claimed technique "wherein the heuristic rule includes information associated with an active networked application making a new connection never previously made."

Appellant respectfully asserts that such excerpts only disclose that a "given application itself can be examined for determining whether it is 'active' by determining whether the application receives

PAGE 31/34 * RCVD AT 11/13/2006 8:36:23 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):11-38

'focus' and/or receives user input," "maintain[ing] a list of active Applications," "each client process can be checked for various characteristics," and "rules which govern Internet access." First, appellant respectfully asserts that such excerpts do not even suggest any sort of heuristic rule, as claimed by appellant. Second, only determining which applications are actively used by a user, as in Freund, clearly does not meet any sort of "information associated with an active networked application making a new connection never previously made," as specifically claimed by appellant (emphasis added).

In the Examiner's Answer mailed 09/11/2006, the Examiner has stated that "[t]he rejection under 35 U.S.C. 112, 1st paragraph for claim 51 is withdrawn." In addition, the Examiner argued that "Freund discloses the applications panel displays a new node for indicating the new executing process and each driver is responsible for monitoring and filtering access for its particular type, including ensuring that any user activity which employs that access type conforms to any rules or conditions specified for the Internet monitor (col.23, lines 20-23 and 52-55)." Further, the Examiner stated that "[t]his recitation reads on the claimed the information associated with an active networked application making a new connection never previously made."

Appellant respectfully disagrees with the Examiner and asserts that Freund merely discloses that "the applications panel 610 (now 610c) displays a new node 613, for indicating the new executing process" (Col. 23, lines 20-21 – emphasis added), and that "[e]ach driver is responsible for monitoring and filtering access for its particular type, including ensuring that any user activity which employs that access type conforms to any rules or conditions specified for the Internet monitor" (Col. 23, lines 52-55 – emphasis added). However, the mere disclosure of the application panel indicating the new executing process fails to suggest "an active networked application making a new connection never previously made" (emphasis added), in the manner as claimed by appellant. Further, the suggestion of the driver responsible for monitoring and filtering access ensures that user activity conforms to any rules or conditions fails to meet appellant's claimed technique "wherein the heuristic rule includes information associated with an active networked application making a new connection never previously made" (emphasis added), as claimed by appellant.

In view of the above, appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met.

PAGE 32/34 * RCVD AT 11/13/2006 8:36:23 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):11-38

Issue # 3:

The Examiner has rejected Claims 13, 27, 41, 49 under 35 U.S.C. 103(a) as being unpatentable over Freund in view of Kaler et al. in view of Official Notice. Appellant respectfully asserts that such claims are not met by the prior art for the reasons argued above with respect to Issue #2, Group #1.

Again, appellant again respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

PAGE 33/34 * RCVD AT 11/13/2006 8:36:23 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):11-38

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P345/01.239.01).

Respectfully submitted,

By: _____ Date: 11/13/06

Kevin J. Zilka
Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660

PAGE 34/34 * RCVD AT 11/13/2006 8:36:23 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/4 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):11-38